Annexe Données personnelles

Version 8.8, 29 octobre 2026, annexe aux Conditions Générales de Service WhoHeld

Entre le **Client** identifié au Bon de commande **et WhoHeld**, société par actions simplifiée unipersonnelle, 49 cours Mirabeau, 13100 Aix-en-Provence, France, RCS Aix-en-Provence 130 164 783 (ci-après « **l'Éditeur** »).

Cette annexe fait partie intégrante du Contrat et **prévaut** sur les CGS en cas de contradiction sur le traitement des données à caractère personnel.

La documentation de conformité de l'Éditeur (qualification, mise en balance, durées, analyse d'impact, diligence sur la source, mesures de sécurité) fait l'objet d'un **dossier de conformité**, remis au Client sur demande sous accord de confidentialité. Il n'est pas contractuel.

Préambule : deux régimes

L'Éditeur ne demande aucun accès au compte Seller Central ou Vendor Central du Client et n'en reçoit aucune donnée : la collecte est faite depuis l'extérieur. Il en résulte deux régimes distincts.

	Objet	Qualité de l'Éditeur
A	Données de marché et de vendeurs tiers	**Responsable de traitement**, pour son propre compte
B	Comptes Utilisateurs, sécurité, facturation	**Sous-traitant** pour l'administration des comptes ; **responsable distinct** pour la sécurité, la journalisation et la mesure d'usage

---

Partie I. Ce que l'Éditeur ne traite pas

L'Éditeur **ne collecte pas et ne reçoit pas** : de données issues du compte marchand du Client ; de données d'acheteurs ou de consommateurs finaux (identités, adresses de livraison, coordonnées, historiques d'achat, contenus de commande) ; de données de paiement de leurs clients ; de catégories particulières de données au sens de l'article 9, ni de données relatives à des condamnations pénales (article 10).

Le Client s'interdit de verser de telles données dans la Plateforme ; son paramétrage (catalogue déclaré, catégories suivies, rôles attribués aux vendeurs) n'en comporte aucune. Si une telle donnée est néanmoins saisie, notamment dans une question posée à Ask WhoHeld, l'Éditeur la supprime ou la masque dès qu'il en a connaissance ; à défaut, elle est effacée par la purge du journal de l'assistant, au plus tard douze (12) mois après son enregistrement. Le Client porte cette interdiction à la connaissance de ses Utilisateurs. **Cet**

engagement est contractuel : toute évolution du produit conduisant l'Éditeur à traiter des données d'acheteurs ferait l'objet d'un avenant incluant un contrat de sous-traitance conforme à l'article 28.

Partie II. Régime A : données de marché et de vendeurs tiers

A.1 Qualité de l'Éditeur

L'Éditeur est responsable de traitement au sens de l'article 4.7 du RGPD. Les Parties constatent qu'il détermine seul les sources, la cadence de l'observation, les méthodes de calcul et les durées ; que la collecte est mutualisée entre ses clients ; que la base d'observation préexiste à l'entrée en relation avec un Client et lui survit ; qu'il assume seul l'information des personnes et le traitement de leurs demandes ; que le Client n'accède ni aux moyens de collecte, ni aux sources, ni aux données telles qu'acquises, mais à des Résultats d'analyse qu'il consulte dans la Plateforme, seuls les livrables de synthèse lui étant remis sous forme de document.

La sélection par le Client de son périmètre, et les rôles qu'il attribue aux vendeurs qu'il observe, s'exercent parmi des possibilités préexistantes et **ne portent que sur la restitution qui lui est faite** : sans effet sur les sources, les méthodes, les durées ni les finalités du traitement, que l'Éditeur détermine seul. La déclaration par le Client de ses propres références de catalogue peut conduire l'Éditeur à observer des références qui ne l'étaient pas encore ; **cette déclaration désigne des objets à observer au sein d'un traitement dont l'Éditeur détermine seul tous les moyens (source, champs, méthodes, cadence réelle, durées) et toutes les finalités** ; les Parties considèrent qu'elle ne constitue pas une codétermination des finalités et des moyens au sens de l'article 26, sous réserve de la qualification résultant des circonstances de fait, l'article A.2 s'appliquant si une responsabilité conjointe était retenue. **La « cadence de collecte engagée » que le Bon de commande fixe (articles 1.1 et 4 des CGS) est un niveau de service commercial (le nombre minimal d'observations garanti au Client pour son Périmètre) et non une instruction du Client sur les moyens de la collecte** : elle ne porte, elle aussi, que sur la restitution qui lui est faite, jamais sur la méthode, le calendrier réel ou la mutualisation de la collecte entre Clients.

A.2 Clause subsidiaire

La qualification résulte des circonstances de fait, non de la seule volonté des Parties. **Si une autorité de contrôle ou une juridiction retenait une responsabilité conjointe, le présent article vaut accord au sens de l'article 26.1** : l'**Éditeur** assume l'information des personnes (art. 13 et 14), toutes les demandes d'exercice de droits (art. 15 à 22), la sécurité (art. 32), la documentation, la notification des violations (art. 33 et 34) et l'analyse d'impact (art. 35) ; le **Client** assume la licéité de l'usage qu'il fait des Résultats et la suppression prévue à l'article A.4. En pareil cas, l'Éditeur met l'essentiel de cet accord à la disposition des personnes concernées dans la notice publiée à https://whoheld.com/trust/sellers-notice (art. 26.2). Le point de contact des personnes reste l'Éditeur, sans préjudice de l'article 26.3.

A.3 Base légale, information, durées

Le traitement repose sur l'**intérêt légitime** (art. 6.1.f), après une mise en balance en trois temps décrite dans le dossier de conformité.

Les données étant collectées indirectement, l'Éditeur publie et maintient à https://whoheld.com/trust/sellers-notice, **à compter du 1er octobre 2026**, une **notice gratuite et librement accessible** portant toutes les mentions des articles 14.1 et 14.2, dont la source, **les durées de conservation** et **le droit d'opposition**, en français, anglais, allemand, espagnol et italien, la version anglaise s'adressant aussi aux vendeurs des places de marché situées hors d'Europe. Les durées appliquées sont celles publiées dans cette notice et dans la Politique de confidentialité.

Le traitement comporte un **profilage** (art. 4.4) limité à l'activité de vente exercée à destination du public. **Aucun Résultat n'est conçu pour constituer, à lui seul ou de manière déterminante, le fondement d'une décision produisant des effets juridiques à l'égard d'un vendeur personne physique ou l'affectant de manière significative** (art. 22, tel qu'interprété par la CJUE dans l'arrêt *SCHUFA*, C-634/21) ; la Plateforme n'exécute aucune décision automatisée, et le Client s'interdit d'utiliser un Résultat comme fondement exclusif ou déterminant d'une telle décision sans analyse préalable de conformité.

A.4 Droits des vendeurs

L'Éditeur traite directement les demandes des vendeurs, sans intervention du Client. **L'opposition est exercée sans frais et sans autre condition que l'invocation de raisons tenant à la situation particulière de la personne** (art. 21.1) ; à sa demande, le traitement est limité pendant l'examen (art. 18.1.d). L'Éditeur ne poursuit que s'il **démontre** des motifs légitimes et impérieux prévalant sur les droits de la personne, ou la nécessité du traitement pour la constatation, l'exercice ou la défense de droits en justice. À défaut, il cesse le traitement, efface les données nominatives, empêche leur réintroduction lors des collectes suivantes et **notifie l'effacement à chacun de ses destinataires** (art. 19), c'est-à-dire à ses clients, seuls destinataires auxquels il restitue des Résultats ; l'effacement chez ses sous-traitants d'hébergement résulte de la suppression en base, et les autorités saisies sur réquisition ne sont pas des destinataires au sens de cette notification. Les mentions de la dénomination du vendeur dans les questions posées par les Utilisateurs à Ask WhoHeld et dans les réponses conservées au journal de cet assistant sont masquées dès l'inscription de l'opposition, puis à chaque passe de maintenance, et supprimées au plus tard douze (12) mois après leur enregistrement, par la purge de ce journal.

Obligation du Client. Le Client ne traite aucune demande de vendeur : il la transmet à l'Éditeur sans y répondre. Sur notification écrite de l'Éditeur identifiant le vendeur concerné, le Client cesse d'utiliser sa dénomination dans ses restitutions et supprime les données nominatives correspondantes **des systèmes actifs et structurés dans lesquels il les exploite**, dans un délai de **soixante (60) jours**.

Relais à ses propres destinataires. L'article 3.3 des CGS autorise le Client à communiquer des Résultats aux sociétés de son groupe, à ses conseils, à ses agences et prestataires de vente en ligne et à ses interlocuteurs au sein des places de marché, sous forme de Résultats traités, jamais les données brutes ni de quoi les reconstituer, et sous une confidentialité équivalente. **L'Éditeur ne connaît pas ces destinataires** : sa notification s'arrête aux siens. Lorsqu'il a communiqué les Résultats concernés, **le Client relaie l'information à ceux de ses destinataires auxquels il les a transmis**, dans le même délai, lorsque ce relais est raisonnablement possible au regard des enregistrements dont il dispose **et dans la mesure où les Résultats concernés permettent encore d'identifier le vendeur**. Un Résultat agrégé, anonymisé ou intégré à une synthèse ne permettant plus cette identification n'appelle aucun relais.

Portée des deux obligations qui précèdent. Elles visent les données que le Client exploite. Les sauvegardes et journaux soumis à un cycle de purge automatique n'ont pas à être modifiés un à un, à condition que les données y soient effacées à l'issue de leur cycle et ne soient ni restaurées ni réutilisées entre-temps. Pour une archive conservée hors de ce cycle, un document déjà diffusé ou un export ancien, le Client apprécie **au cas par cas** si l'une des exceptions de l'article 17, paragraphe 3, du RGPD s'applique, notamment une obligation légale de conservation ou la constatation, l'exercice ou la défense de droits en justice ; à défaut, il les traite comme les données qu'il exploite, et à tout le moins en limite l'usage. Le Client répercute de la même façon toute rectification ou limitation du traitement que l'Éditeur lui notifie (article 19 du RGPD). Ces obligations prennent fin trente-six (36) mois après la fin du Contrat, terme de la conservation des séries rattachées à un vendeur.

A.5 Conséquence pour le Client

L'Éditeur assume la documentation de la base d'observation : le registre, la mise en balance, l'analyse d'impact, l'information des personnes et le traitement de leurs demandes. Sous la seule réserve de l'article A.4, il n'attend rien du Client à ce titre : celui-ci reçoit un résultat d'analyse, pas un traitement délégué. **Le Client répond en revanche de l'usage qu'il fait des Résultats.** Lorsqu'ils comportent des données relatives à des vendeurs personnes physiques et qu'il les exploite dans ses propres traitements (documents, outils, décisions commerciales), il en est responsable de traitement pour cet usage : il le documente dans son propre registre (article 30 du RGPD) et en assure la licéité (articles 5 et 24).

Partie III. Régime B : comptes Utilisateurs, sécurité et facturation

L'Éditeur est **sous-traitant** (art. 28) pour la création, la gestion et la suppression des comptes Utilisateurs, l'attribution des droits, l'authentification, le support et l'envoi des alertes demandées. Il est **responsable de traitement distinct**, sur le fondement de son intérêt légitime (art. 6.1.f) et, pour la facturation, de ses obligations légales et contractuelles, pour la sécurité du service, la journalisation et sa conservation, l'investigation des incidents, la mesure d'usage nécessaire à la facturation, au contrôle de l'article 4 des CGS et au pilotage de l'accompagnement du Client (pages consultées, agrégées par compte client), la production de statistiques agrégées et anonymisées, et l'**accompagnement de l'évaluation gratuite** (CGS 1.5 : échanges avec les Utilisateurs, indicateurs d'usage pendant l'évaluation, série de messages d'accompagnement, preuve de l'acceptation des conditions de l'évaluation). Le Client **informe ses Utilisateurs** de cette seconde qualité (art. 13), par renvoi à la Politique de confidentialité de l'Éditeur.

B.1 Description du traitement de sous-traitance (article 28.3)

Objet	Création, gestion et sécurisation des accès des Utilisateurs désignés par le Client
Nature	Hébergement, authentification, attribution des droits, support
Finalité	Permettre aux Utilisateurs du Client d'accéder à la Plateforme
Durée	Durée du Contrat, puis fenêtre de réversibilité de l'article 12 des CGS
Personnes concernées	Salariés du Client et prestataires agissant pour les seuls besoins du Client, à l'exclusion des agences servant d'autres clients, désignés comme Utilisateurs

Données	Nom, prénom, adresse électronique professionnelle, entreprise, rôle et droits ; références produits consultées via l'extension, aux seules fins d'affichage et sans journalisation

Les identifiants techniques, adresses IP, horodatages de connexion et journaux d'activité relèvent du traitement de sécurité, pour lequel l'Éditeur est responsable.

B.2 Obligations de l'Éditeur en qualité de sous-traitant

a) Traiter les données **sur instruction documentée** du Client (Contrat, présente annexe et paramétrage valent instructions), et l'informer immédiatement si une instruction lui paraît violer le RGPD. **b)** Garantir la **confidentialité** : les personnes habilitées sont tenues d'une obligation contractuelle ou légale. **c)** Mettre en œuvre et maintenir les **mesures techniques et organisationnelles** décrites à l'**annexe Sécurité** ci-après (art. 32), et les faire évoluer selon l'état de l'art. **d)** Respecter les conditions de **sous-traitance ultérieure** de l'article C.1. **e) Assister le Client** pour les demandes d'exercice de droits (le retrait d'un Utilisateur est disponible dans la Plateforme par l'administrateur du Client, hors évaluation gratuite, ou sur demande écrite à l'Éditeur : le compte retiré est bloqué au plus tard le jour ouvré suivant la demande, ses sessions sont révoquées, puis il est supprimé sous trente (30) jours ; l'export et la rectification des données d'un compte sont réalisés sur demande), la sécurité, la notification des violations et, le cas échéant, l'analyse d'impact (art. 32 à 36) ; lui transmettre toute demande reçue directement **sans y répondre**. Les fonctions en libre-service de la Plateforme et la documentation mise à disposition sont fournies sans frais ; **l'assistance qui va au-delà est facturée au temps passé**, au tarif en vigueur, sauf si elle est rendue nécessaire par un manquement de l'Éditeur. **f) Notifier toute violation de données** au Client sans délai injustifié et, **si possible, dans les quarante-huit (48) heures** de sa connaissance, par écrit et de façon datable, en précisant la nature de la violation, les catégories et le nombre approximatif de personnes et d'enregistrements, les conséquences probables, les mesures prises et le point de contact ; une information préliminaire est transmise dès la connaissance de l'événement, même incomplète. **g) Mettre à disposition la documentation** nécessaire pour démontrer le respect de l'article 28 et permettre l'audit de l'article C.3. **h) Tenir le registre** des catégories d'activités effectuées pour le compte du Client (art. 30.2). **i) Ne pas utiliser ces données pour ses propres finalités**, sous réserve des traitements pour lesquels il est responsable au titre du présent régime et des statistiques agrégées et anonymisées au sens du considérant 26 : aucune personne individualisable, aucun enregistrement corrélable, aucune information inférable.

B.3 Sort des données au terme du Contrat

Le sort des données au terme du Contrat, y compris en cas de changement de prestataire, suit l'**article 12 des CGS**, dont les délais ne sont pas répétés ici. En substance : le Client récupère les **Données Client qu'il a saisies** dans la Plateforme (catalogue déclaré, déclarations, rôles attribués aux vendeurs, paramétrage), dans un format structuré et couramment utilisé ; les données de marché relèvent du régime A et ne font l'objet d'aucun export ; les livrables de synthèse déjà remis (revue mensuelle, dossier de négociation, rapport d'événement) restent utilisables pour son usage interne. Au terme de la période de récupération prévue à l'article 12 des CGS, les comptes Utilisateurs et les Données Client sont supprimés des environnements de production, puis des sauvegardes selon un cycle de rotation n'excédant pas quatre-vingt-dix (90) jours. **Attestation écrite de suppression** remise sur demande. Seules sont conservées les données nécessaires au respect d'une obligation légale, pour la durée prescrite et sous le même régime de sécurité.

Partie IV. Stipulations communes

C.1 Sous-traitants ultérieurs

Le Client autorise les sous-traitants listés à l'annexe 1. L'Éditeur l'informe de tout ajout ou remplacement **au moins quinze (15) jours** avant sa mise en œuvre ; le Client peut s'y opposer dans les dix (10) jours pour un motif raisonnable tenant à la protection des données ; à défaut d'accord dans les trente (30) jours, il peut résilier sans indemnité, avec remboursement au prorata temporis. L'Éditeur impose à chaque sous-traitant des obligations au moins équivalentes et **demeure pleinement responsable envers le Client**.

C.2 Localisation et transferts

Les données sont hébergées **au sein de l'Union européenne** (annexe 1), à une exception près : Resend, société établie aux États-Unis, envoie les messages depuis l'Irlande mais **stocke aux États-Unis** les données des messages (adresse du destinataire, contenu, journal d'envoi). Les autres sous-traitants établis hors de l'Union, Supabase Pte. Ltd. (Singapour), Vercel Inc. et Functional Software, Inc. (Sentry) (États-Unis), peuvent accéder depuis ces pays aux données qu'ils traitent. Anthropic Ireland, Limited, établie en Irlande, fait traiter les données aux États-Unis par sa société mère Anthropic, PBC. Anthropic reçoit des données pseudonymisées issues des Résultats et, le cas échéant, les données que l'Utilisateur saisit librement dans sa question à Ask WhoHeld ; ce flux constitue un transfert de données à caractère personnel vers les États-Unis ; Anthropic efface les questions et les réponses de ses systèmes sous trente (30) jours, sauf conservation plus longue imposée par la loi ou, jusqu'à deux (2) ans, lorsqu'un échange est signalé comme contraire à sa politique d'utilisation, et ne les utilise pas pour entraîner ses modèles (conditions commerciales d'Anthropic, relevées le 29/10/2026 ; toute modification défavorable est traitée selon l'article C.1). Ces transferts sont encadrés par les clauses contractuelles types de la décision d'exécution (UE) 2021/914, intégrées à leurs contrats de sous-traitance. Google Cloud France SARL, 8 rue de Londres, 75009 Paris (Google Workspace), établie dans l'Union, ne permet pas de choisir la région de stockage des données dans la formule souscrite : les échanges de messagerie peuvent être traités dans des centres de données de Google situés hors de l'Union, transferts encadrés par l'avenant de traitement des données de Google Cloud (clauses contractuelles types de la décision d'exécution (UE) 2021/914 ; Google LLC est certifiée au cadre de protection des données UE–États-Unis). Tout autre transfert vers un pays tiers est subordonné à une décision d'adéquation en vigueur à la date du transfert ou, à défaut, aux clauses contractuelles types de la décision d'exécution (UE) 2021/914, assorties d'une analyse d'impact du transfert et des mesures supplémentaires appropriées.

Sociétés du groupe du Client établies hors de l'Espace économique européen. Lorsque l'Éditeur accepte la désignation d'une société du groupe du Client établie hors de l'Espace économique européen et du Royaume-Uni (article 3.1 des CGS), la consultation par ses Utilisateurs de Résultats comportant des données de vendeurs constitue un transfert de l'Éditeur, responsable du régime A, vers cette société, responsable de son propre usage. Ce transfert n'a lieu que si le pays de cette société bénéficie d'une décision d'adéquation, ce qui inclut une société établie aux États-Unis et certifiée au cadre de protection des données UE–États-Unis, ou, à défaut, si cette société a souscrit avant tout accès les clauses contractuelles types de la décision d'exécution (UE) 2021/914, module 1 (de responsable à responsable), que l'Éditeur fournit, assorties d'une analyse d'impact du transfert.

Places de marché hors de l'Union. L'observation de vendeurs présents sur des places de marché situées hors de l'Union (Royaume-Uni, États-Unis, Canada, Japon, Mexique, Brésil, Inde) **ne constitue pas un transfert hors de l'Union** : les données sont collectées vers l'Union et y sont hébergées. Un transfert sortant vers un prestataire établi au Royaume-Uni serait soumis à la décision d'adéquation en vigueur ou, à défaut, aux clauses types assorties de l'addendum britannique.

C.3 Audit

Le Client peut vérifier le respect de la partie III **une fois par période de douze (12) mois**, moyennant un préavis écrit de **soixante (60) jours**, par la communication du **dossier de conformité** : description des mesures, attestations et rapports des sous-traitants d'infrastructure, réponses à un questionnaire de sécurité.

Audit sur site, en dernier recours (article 28.3.h du RGPD). Il n'a lieu que si le dossier de conformité ne suffit pas à établir le respect de la partie III au regard d'un risque **précis et identifié par écrit**, ou sur injonction d'une autorité de contrôle. Il est conduit par un auditeur indépendant mandaté par le Client, **tenu au secret** et **non concurrent** de l'Éditeur, moyennant un préavis écrit de **trente (30) jours**, aux heures ouvrées et **dans la limite d'une (1) journée**.

L'audit ne peut porter sur les données d'autres clients. Il est **aux frais du Client**, y compris le temps que l'Éditeur y consacre, facturé au temps passé au tarif en vigueur, sauf s'il révèle un manquement substantiel de l'Éditeur. Une fréquence supérieure est admise à la demande d'une autorité ou après une violation avérée. Le régime A n'est pas soumis à l'audit du Client, l'Éditeur y agissant pour son propre compte, **sauf application de l'article A.2**, auquel cas le Client peut obtenir les éléments nécessaires à ses obligations propres au titre de l'article 26.

C.4 Responsabilité

La responsabilité respective des Parties est régie par l'article 82 du RGPD. **Le droit d'une personne concernée d'obtenir réparation de son entier préjudice auprès de l'une ou l'autre Partie (article 82, paragraphes 1 et 4) n'est en rien limité par le Contrat.** Entre les Parties seulement, les recours prévus à l'article 82, paragraphe 5, sont limités, conformément à l'article 13.3 des CGS, au **double du plafond de l'article 13.2 des CGS** et, pendant l'évaluation gratuite, à **deux mille (2 000) euros** (article 1.5 des CGS). Ces limites ne jouent pas dans les cas où ces articles les écartent (dol, faute lourde).

C.5 Contacts

	Client	**Éditeur**
Contact protection des données	*(indiqué au Bon de commande, section A)*	privacy@whoheld.com

C.6 Cessation d'activité et transmission

En cas de **cessation d'activité**, les données du régime A sont supprimées dans les quatre-vingt-dix (90) jours, sous réserve des obligations légales ; celles du régime B suivent l'article 12.4 des CGS, qui prévaut alors sur l'article B.3.

En cas de **cession, d'apport ou de fusion** emportant transmission de la base d'observation, le cessionnaire est tenu, par l'acte de cession, des mêmes finalités, durées et limitations. Les personnes

concernées en sont informées par la mise à jour de la notice https://whoheld.com/trust/sellers-notice **préalablement à la reprise du traitement**, et peuvent s'y opposer à cette occasion.

Annexe 1. Sous-traitants ultérieurs

Liste au 27 octobre 2026. Version à jour à https://whoheld.com/trust#subprocessors.

Sous-traitant	Rôle	Régime	Localisation du traitement
Supabase Pte. Ltd. (infrastructure Amazon Web Services)	Base de données, authentification, stockage	A et B	**France, région AWS** `eu-west-3` **(Paris)** ; société établie à Singapour, équipes réparties dans le monde, clauses contractuelles types (UE) 2021/914
Hostinger International Ltd.	Serveur d'exécution de la collecte	A et B	France (Paris), Union européenne ; sauvegardes hebdomadaires de l'instance aux Pays-Bas, Union européenne *(Union européenne, voir note ci-dessous)*
Resend	Messages de service, alertes et série d'accompagnement de l'évaluation	A et B	Envoi depuis l'Irlande (région eu-west-1) ; **données des messages stockées aux États-Unis** ; société établie aux États-Unis, clauses contractuelles types (UE) 2021/914
Anthropic Ireland, Limited (Irlande ; traitement aux États-Unis par sa société mère Anthropic, PBC)	Analyse assistée par intelligence artificielle (Ask WhoHeld : réponses aux questions des Utilisateurs), sur données pseudonymisées et sur la question saisie par l'Utilisateur	A et B	**États-Unis** ; clauses contractuelles types (UE) 2021/914
Vercel Inc.	Hébergement de l'application web	A et B	Allemagne (Francfort, région fra1), réseau de diffusion mondial ; société établie aux États-Unis, clauses contractuelles types (UE) 2021/914
Functional Software, Inc. (Sentry), San Francisco	Remontée des erreurs techniques de l'application web, pour diagnostiquer et corriger les pannes : message et pile d'erreur caviardés, identifiant technique du compte Utilisateur et du Client, page concernée, navigateur, système d'exploitation, type	B	**Allemagne (Francfort)**, région de données de l'Union de Sentry ; société établie aux États-Unis, d'où des accès sont possibles (support, métadonnées de compte) :

Sous-traitant	Rôle	Régime	Localisation du traitement
	d'appareil, langue et fuseau horaire déclarés par le navigateur ; jamais d'adresse électronique, de mot de passe ou de jeton, de contenu de requête ni d'identifiant de vendeur ; aucune adresse IP conservée et aucune géolocalisation, y compris déduite de l'adresse IP ; conservation quatre-vingt-dix (90) jours au plus		cadre de protection des données UE–États-Unis et, à défaut, clauses contractuelles types (UE) 2021/914 (avenant de traitement des données de Sentry)
Scaleway SAS, Paris	Stockage de la copie de sauvegarde hebdomadaire chiffrée et de la copie quotidienne chiffrée des journaux de sécurité du serveur d'exécution (annexe 2) : les copies sont chiffrées avant leur envoi, et ce sous-traitant ne détient pas la clé qui permettrait de les lire ; elles ne contiennent ni mot de passe ni second facteur d'authentification ; conservation quatre-vingt-dix (90) jours	A et B	France (Paris, région fr-par), Union européenne ; société établie en France, aucun transfert hors de l'Union
Google Cloud France SARL, 8 rue de Londres, 75009 Paris (Google Workspace)	Messagerie professionnelle de l'Éditeur : échanges avec le Client et ses Utilisateurs, invitations, support et accompagnement de l'évaluation	A et B	Centres de données de Google, sans choix de région dans la formule souscrite : transferts possibles hors de l'Union européenne, encadrés par l'avenant de traitement des données de Google Cloud (Cloud Data Processing Addendum : clauses contractuelles types (UE) 2021/914 ; Google LLC certifiée au cadre de protection des données UE–États-Unis)

Hostinger propose des instances hors Union européenne (notamment États-Unis, Singapour, Brésil) en plus d'instances européennes : l'engagement de l'article C.2 (« Les données sont hébergées au sein de l'Union européenne ») ne vaut pour ce sous-traitant que si l'instance effectivement utilisée est confirmée en zone UE. Cette localisation est vérifiée et consignée **avant toute mise en production, y compris pour une évaluation gratuite**, et à chaque changement d'instance, selon la procédure de l'article C.1 ; à défaut de confirmation UE, ce sous-traitant est retiré des régimes A et B jusqu'à correction. L'instance utilisée est à Paris ; ses sauvegardes hebdomadaires sont stockées par Hostinger aux Pays-Bas, également dans l'Union : aucun transfert hors de l'Union n'en résulte.

Aucun outil tiers de mesure d'audience n'est déployé à la date de la présente version ; s'il en était installé un, il serait ajouté selon la procédure de l'article C.1. La liste est mise à jour à chaque ajout ou remplacement, selon cette même procédure.

Annexe 2. Sécurité

Mesures techniques et organisationnelles au sens de l'article 32 du RGPD. **Cette annexe fait partie du Contrat.** L'Éditeur ne peut la modifier que dans un sens équivalent ou supérieur, dans les conditions de l'article 7.2 des CGS.

Contrôle d'accès. Accès nominatifs, aucun compte partagé, moindre privilège. **Authentification multifacteur sur les accès d'administration et les consoles des sous-traitants d'infrastructure, mise en œuvre avant toute ouverture d'accès au Client, y compris au titre d'une évaluation gratuite** : tout privilège d'administration de la Plateforme exige un second facteur vérifié pendant la session, contrôlé par la base comme par l'application. Cloisonnement des données entre clients **au niveau de la base** (isolation par politique de sécurité au niveau des lignes, propre à chaque client) et non seulement de l'application, vérifié chaque jour par des contrôles automatisés des droits d'accès et des données servies : l'Éditeur met en œuvre ces moyens pour qu'une erreur applicative n'expose pas les données d'un autre client. **Fait exception le référentiel des vendeurs observés**, commun à l'ensemble des clients : il ne comporte aucune Donnée Client et relève du régime A. Séparation des rôles techniques ; clés d'administration jamais exposées à l'application cliente. Revue des habilitations et révocation à la sortie d'un collaborateur.

Chiffrement. TLS 1.2 minimum en transit ; chiffrement au repos assuré par l'infrastructure d'hébergement ; secrets et clés hors du code source, aucune clé en clair dans un dépôt.

Journalisation et supervision. Journalisation des opérations d'administration sensibles : ouverture, prolongation, fermeture et conversion des accès, invitations, retraits et changements de rôle des Utilisateurs, passage d'un administrateur de l'Éditeur à la vue d'un client. Les connexions sont journalisées par le fournisseur d'authentification, pour la durée de conservation de son offre. Supervision continue de la production, avec alerte sur **absence de signal** : le silence du système déclenche l'alerte, il n'est jamais lu comme un fonctionnement normal. Journaux conservés selon les durées publiées, alignées sur les purges programmées ; les journaux de sécurité du serveur d'exécution sont en outre copiés chaque jour hors de ce serveur, chiffrés et verrouillés quatre-vingt-dix (90) jours (Scaleway SAS, annexe 1).

Sauvegardes. Automatiques et quotidiennes ; profondeur de restauration effective = celle du palier souscrit auprès de l'hébergeur, communiquée sur demande ; suppression au terme d'un cycle de rotation n'excédant pas quatre-vingt-dix jours. Une **copie hebdomadaire** des données que la collecte et le calcul ne reconstituent pas (comptes, accès, déclarations, décisions et journaux) est en outre déposée chez un prestataire distinct de l'hébergeur de la base (Scaleway SAS, annexe 1) : chiffrée avant son envoi, avec une clé dont la partie privée n'est conservée ni sur le serveur qui la produit ni chez ce prestataire ; conservée quatre-vingt-dix (90) jours, sous un verrou qui interdit à quiconque, l'Éditeur compris, de l'effacer ou de la modifier avant cette échéance. Une suppression faite dans la base n'atteint une copie déjà déposée qu'à l'échéance de son verrou. Un **test de restauration daté et documenté est exécuté au plus tard à la date d'effet du premier Bon de commande**, puis périodiquement.

Développement et exploitation. Tests automatisés à chaque modification, en intégration continue ; un échec est traité avant toute mise en production. Un contrôle automatisé vérifie les droits d'accès à la base après toute modification du schéma ou des habilitations et échoue si un droit client est cassé. Accès à la production restreints aux personnes habilitées, depuis des postes maîtrisés. **Un environnement de test séparé de la production, sans donnée de production, est en service depuis le 26 octobre 2026** : toute modification du schéma de la base y est appliquée avant de l'être en production. Revue de

sécurité interne périodique et documentée ; test d'intrusion externe lorsque le Bon de commande le prévoit.

Incidents. Procédure de qualification, confinement, correction ; notification au client sans délai injustifié, si possible dans les quarante-huit heures de la connaissance d'une violation ; **registre interne des violations** (article 33.5), y compris non notifiées ; analyse post-incident documentée.

Personnel. Engagement de confidentialité, sensibilisation, révocation des accès en fin de mission.

Une description actualisée figure dans le dossier de conformité, communiqué sur demande sous accord de confidentialité.